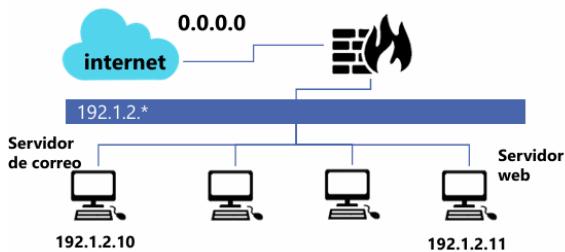


ACTIVIDAD 04 -

Mecanismos de defensa en red.

Teniendo en cuenta la topología de red mostrada completa la tabla con las reglas de iptables que deberían aplicarse en el Firewall para llevar a cabo las acciones solicitadas. Las reglas, siempre que sea posible, deben determinar protocolo, dirección IP origen y destino, puerto/s origen y destino y el estado de la conexión.



1. Establecer una política restrictiva.
2. Permitir el tráfico de conexiones ya establecidas.
3. Aceptar tráfico DNS (TCP) saliente de la red local.
4. Aceptar correo entrante proveniente de Internet en el servidor de correo.
5. Permitir correo saliente a Internet desde el servidor de correo.
6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.
7. Permitir tráfico HTTP desde la red local a Internet.

1. iptable -A INPUT -j DROP
2. iptable -A INPUT -p tcp -m state ESTABLISHED -j ACCEPT
3. iptable -A OUTPUT -p tcp - -sports 53 -j ACCEPT
4. iptable -A INPUT -p tcp -s 192.1.2.10 -d 0.0.0.0 -j ACCEPT
5. iptable -A OUTPUT -p tcp - -s 192.1.2.10 -j ACCEPT
6. iptable -A INPUT -p tcp - -dports 80 -d 192.1.2.11 -s 0.0.0.0 -j ACCEPT
7. iptable -A INPUT -p tcp - -d 0.0.0.0 -j ACCEPT